



Panduan Pengguna

AWS Artifact



AWS Artifact: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS Artifact?	1
Harga	1
Memulai	2
Mendaftar untuk Akun AWS	2
Fitur	2
Mengunduh laporan	3
Mengunduh laporan	3
Melihat lampiran dalam dokumen PDF	4
Mengamankan dokumen Anda	5
Pemecahan masalah	5
Mengelola perjanjian	6
Menerima perjanjian akun	6
Mengakhiri perjanjian akun	8
Menerima perjanjian organisasi	8
Mengakhiri perjanjian organisasi	10
Perjanjian offline	11
Mengkonfigurasi notifikasi	12
Prasyarat	12
Membuat konfigurasi	13
Mengedit konfigurasi	14
Menghapus konfigurasi	15
Manajemen identitas dan akses	16
Memberikan akses pengguna	16
Langkah 1: Buat kebijakan IAM	17
Langkah 2: Buat grup IAM dan lampirkan kebijakan	17
Langkah 3: Buat pengguna IAM dan tambahkan ke grup	18
Contoh kebijakan IAM di Wilayah komersial AWS	18
Contoh kebijakan IAM di AWS GovCloud (US) Regions	36
Menggunakan kebijakan AWS terkelola	47
AWSArtifactReportsReadOnlyAccess	47
AWSArtifactAgreementsReadOnlyAccess	48
AWSArtifactAgreementsFullAccess	48
Pembaruan kebijakan	49
Menggunakan peran tertaut layanan	50

Service-linked izin peran untuk AWS Artifact	51
Membuat peran terkait layanan untuk AWS Artifact	51
Menyunting peran terkait layanan untuk AWS Artifact	52
Menghapus peran terkait layanan untuk AWS Artifact	52
Wilayah yang Didukung untuk AWS Artifact peran terkait layanan	53
Menggunakan tombol kondisi IAM	54
CloudTrail penebangan	57
AWS Artifact informasi di CloudTrail	57
Memahami entri file AWS Artifact log	59
Riwayat dokumen	61
.....	lxvi

Apa itu AWS Artifact?

AWS Artifact menyediakan unduhan dokumen AWS keamanan dan kepatuhan sesuai permintaan. Misalnya, laporan tentang kepatuhan terhadap standar International Organization for Standardization (ISO) dan Payment Card Industry (PCI) Security Standards, dan System and Organization Controls (SOC). AWS Artifact juga menyediakan unduhan sertifikasi dari badan akreditasi yang memvalidasi implementasi dan efektivitas operasi kontrol keamanan. AWS

Dengan AWS Artifact, Anda juga dapat mengunduh dokumen keamanan dan kepatuhan untuk vendor perangkat lunak independen (ISV) yang menjual produk mereka. AWS Marketplace Untuk informasi selengkapnya, lihat [Wawasan AWS Marketplace Vendor](#).

Selain itu, Anda dapat menggunakan AWS Artifact untuk meninjau, menerima, dan melacak status perjanjian Anda dengan AWS untuk Anda Akun AWS dan untuk beberapa Akun AWS di organisasi Anda. Untuk informasi lebih lanjut tentang perjanjian di AWS Artifact, lihat [Mengelola perjanjian di AWS Artifact](#).

Untuk menunjukkan keamanan dan kepatuhan AWS infrastruktur dan layanan yang Anda gunakan, Anda dapat mengirimkan AWS Artifact dokumen kepada auditor atau regulator Anda sebagai artefak audit. Anda juga dapat menggunakan artefak audit ini sebagai pedoman untuk mengevaluasi arsitektur cloud Anda sendiri dan untuk menilai efektivitas kontrol internal perusahaan Anda. Untuk informasi selengkapnya tentang artefak audit, lihat [AWS Artifact FAQ](#).

Note

AWS pelanggan bertanggung jawab untuk mengembangkan atau memperoleh dokumen yang menunjukkan keamanan dan kepatuhan perusahaan mereka. Untuk informasi selengkapnya, lihat [Model Tanggung Jawab Bersama](#).

Harga

AWS memberikan AWS Artifact dokumen dan perjanjian kepada Anda secara gratis.

Memulai dengan AWS Artifact

Untuk mulai menggunakan AWS Artifact, coba fitur utamanya di AWS Artifact konsol. Di konsol, Anda dapat mengunduh laporan AWS keamanan dan kepatuhan, mengunduh dan menerima perjanjian hukum, dan berlangganan pemberitahuan tentang AWS Artifact dokumen.

Mendaftar untuk Akun AWS

Untuk memulai AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat [Memulai dengan Akun AWS](#) di Panduan AWS Account Management Referensi.

Fitur

Untuk petunjuk tentang penggunaan fitur AWS Artifact, lihat topik berikut:

- [Mengunduh laporan](#)
- [Mengelola perjanjian](#)
- [Mengkonfigurasi notifikasi](#)

Mengunduh laporan di AWS Artifact

Anda dapat mengunduh laporan dari AWS Artifact konsol. Saat Anda mengunduh laporan AWS Artifact, laporan dibuat khusus untuk Anda, dan setiap laporan memiliki tanda air yang unik. Maka dari itu, Anda hanya boleh berbagi laporan ini dengan orang-orang yang Anda percaya. Jangan lampirkan laporan dalam email dan jangan bagikan secara online. Untuk membagikan laporan, gunakan layanan berbagi aman seperti Amazon WorkDocs. Beberapa laporan mengharuskan Anda untuk menerima Syarat dan Ketentuan sebelum Anda dapat mengunduhnya.

Daftar Isi

- [Mengunduh laporan](#)
- [Melihat lampiran dalam dokumen PDF](#)
- [Mengamankan dokumen Anda](#)
- [Pemecahan masalah](#)

Mengunduh laporan

Untuk mengunduh laporan, Anda harus memiliki izin yang diperlukan. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di AWS Artifact](#).

Saat Anda mendaftar AWS Artifact, akun Anda secara otomatis diberikan izin untuk mengunduh beberapa laporan. Jika Anda mengalami kesulitan mengakses AWS Artifact, ikuti panduan pada halaman [Referensi Otorisasi AWS Artifact Layanan](#).

Untuk mengunduh laporan

1. Buka AWS Artifact konsol di <https://console.aws.amazon.com/artifact/>.
2. Di halaman AWS Artifact beranda, pilih Lihat laporan.

Pada halaman Laporan, pada tab AWS laporan, Anda dapat mengakses AWS laporan (misalnya, SOC 1/2/3, PCI, C5, dan sebagainya). Pada tab Laporan pihak ketiga, Anda dapat mengakses laporan dari vendor perangkat lunak independen (ISVs) yang menjual produk mereka. AWS Marketplace

3. (Opsional) Untuk menemukan laporan, masukkan kata kunci di bidang pencarian. Anda juga dapat melakukan penelusuran yang ditargetkan untuk laporan berdasarkan kolom individual, termasuk judul laporan, kategori, seri, dan deskripsi. Misalnya, untuk menemukan laporan

Cloud Computing Compliance Controls Catalogue (C5), Anda dapat mencari kolom Judul menggunakan “Judul”, operator “berisi” (:), dan istilah “C5” (). **Title : C5**

4. (Opsional) Untuk informasi lebih lanjut tentang laporan, pilih judul laporan untuk membuka halaman detailnya.
5. (Opsional) Jika ingin mengunduh laporan versi sebelumnya, Anda dapat membuka halaman detail laporan dengan memilih judul laporan. Pada halaman detail, cari bagian Versi sebelumnya, dan di baris versi yang diinginkan, pilih Unduh untuk mengunduh versi laporan tertentu.
6. Pilih laporan, lalu pilih Unduh laporan.
7. Anda mungkin diminta untuk menerima syarat dan ketentuan (Terima persyaratan untuk mengunduh laporan) untuk laporan spesifik yang Anda unduh. Kami menyarankan Anda membaca syarat dan ketentuan dengan cermat. Setelah selesai membaca, pilih Saya telah membaca dan menyetujui persyaratan, lalu pilih Terima persyaratan dan unduh laporan.
8. Buka file yang diunduh melalui penampil PDF. Tinjau syarat dan ketentuan untuk penerimaan dan gulir ke bawah untuk menemukan laporan audit. Laporan dapat memiliki informasi tambahan yang disematkan sebagai lampiran dalam dokumen PDF, jadi pastikan untuk memeriksa lampiran dalam file PDF untuk dokumentasi pendukung. Untuk petunjuk tentang cara melihat lampiran, lihat [Melihat lampiran dalam dokumen PDF](#).

Melihat lampiran dalam dokumen PDF

Kami merekomendasikan aplikasi berikut yang saat ini mendukung tampilan lampiran PDF:

Pembaca Adobe Acrobat

Unduh versi terbaru Adobe Acrobat Reader dari situs web Adobe di <https://get.adobe.com/reader/>.

Untuk petunjuk tentang cara melihat lampiran PDF di Acrobat Reader, lihat [Tautan dan lampiran PDFs di](#) situs web Adobe Support.

Peramban Firefox

1. Unduh browser web Firefox terbaru dari situs web Mozilla di <https://www.mozilla.org/en-US/firefox/new/>.
2. Buka file PDF di penampil PDF bawaan Firefox. Untuk petunjuk, lihat [Melihat file PDF di Firefox atau pilih penampil lain](#) di situs web Dukungan Mozilla.
3. Untuk melihat lampiran PDF di penampil PDF bawaan Firefox, pilih Toggle Sidebar, Tampilkan Lampiran.

Mengamankan dokumen Anda

AWS Artifact Dokumen bersifat rahasia dan harus dijaga keamanannya setiap saat. AWS Artifact menggunakan model tanggung jawab AWS bersama untuk dokumennya. Ini berarti bahwa AWS bertanggung jawab untuk menjaga dokumen tetap aman saat berada di AWS Cloud, tetapi Anda bertanggung jawab untuk menjaganya tetap aman setelah Anda mengunduhnya. AWS Artifact mungkin mengharuskan Anda untuk menerima Syarat dan Ketentuan sebelum Anda dapat mengunduh dokumen. Setiap unduhan dokumen memiliki watermark unik yang dapat dilacak.

Anda hanya diizinkan untuk berbagi dokumen yang ditandai sebagai dokumen rahasia dengan lingkaran dalam perusahaan Anda, dengan regulator Anda, dan dengan auditor Anda. Anda tidak diizinkan untuk berbagi dokumen ini dengan pelanggan Anda atau di situs web Anda. Kami sangat menyarankan Anda menggunakan layanan berbagi dokumen yang aman, seperti Amazon WorkDocs, untuk berbagi dokumen dengan orang lain. Jangan mengirim dokumen melalui email atau mengunggahnya ke situs yang tidak aman.

Pemecahan masalah

Jika Anda tidak dapat mengunduh dokumen atau menerima pesan kesalahan, lihat [Pemecahan Masalah](#) di FAQ AWS Artifact .

Mengelola perjanjian di AWS Artifact

Anda dapat menggunakan AWS Artifact untuk meninjau dan mengelola perjanjian untuk Anda Akun AWS atau organisasi. Misalnya, perusahaan yang tunduk pada Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) biasanya memerlukan perjanjian Business Associate Addendum (BAA) AWS untuk memastikan bahwa informasi kesehatan yang dilindungi (PHI) dilindungi dengan tepat. Di AWS Artifact konsol, Anda dapat meninjau dan menerima perjanjian tersebut, dan Anda dapat menunjuk sebuah Akun AWS yang dapat memproses PHI secara legal.

Jika Anda menggunakan AWS Organizations, Anda dapat menerima perjanjian, seperti BAA dengan AWS, atas nama semua Akun AWS di organisasi Anda. Semua akun anggota yang ada dan selanjutnya secara otomatis tercakup dalam perjanjian dan dapat memproses PHI secara legal.

Anda juga dapat menggunakan AWS Artifact untuk mengonfirmasi bahwa Anda Akun AWS atau organisasi telah menerima perjanjian, dan untuk meninjau ketentuan perjanjian yang diterima untuk memahami kewajiban Anda. Jika akun atau organisasi Anda tidak lagi perlu menggunakan perjanjian yang diterima, maka Anda dapat menggunakannya AWS Artifact untuk mengakhiri perjanjian. Jika Anda mengakhiri perjanjian tetapi kemudian menyadari bahwa Anda membutuhkannya, maka Anda dapat mengaktifkan perjanjian lagi.

Daftar Isi

- [Menerima perjanjian untuk Anda Akun AWS di AWS Artifact](#)
- [Mengakhiri perjanjian untuk Anda Akun AWS di AWS Artifact](#)
- [Menerima perjanjian untuk organisasi Anda di AWS Artifact](#)
- [Mengakhiri perjanjian untuk organisasi Anda di AWS Artifact](#)
- [Perjanjian offline di AWS Artifact](#)

Menerima perjanjian untuk Anda Akun AWS di AWS Artifact

Anda dapat menggunakan AWS Artifact konsol untuk meninjau dan menerima perjanjian dengan AWS untuk Anda Akun AWS.

Important

Sebelum Anda menerima perjanjian, sebaiknya Anda berkonsultasi dengan tim legal, privasi, dan kepatuhan Anda.

Izin yang diperlukan

Jika Anda adalah administrator akun, Anda dapat memberikan izin kepada pengguna IAM dan pengguna gabungan untuk mengakses dan mengelola satu atau beberapa perjanjian Anda. Secara default, hanya pengguna dengan hak administratif yang dapat menerima perjanjian. [Untuk menerima perjanjian, IAM dan pengguna federasi harus memiliki izin yang diperlukan.](#)

Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di AWS Artifact](#).

Untuk menerima perjanjian dengan AWS

1. Buka AWS Artifact konsol di <https://console.aws.amazon.com/artifact/>.
2. Pada panel AWS Artifact navigasi, pilih Perjanjian.
3. Pilih tab Perjanjian akun.
4. Buka AWS Artifact konsol di <https://console.aws.amazon.com/artifact/>.
5. Di panel navigasi, pilih Perjanjian.
6. Pada halaman Perjanjian, lakukan salah satu hal berikut:
 - Untuk menerima perjanjian hanya untuk akun Anda, pilih tab Perjanjian akun.
 - Untuk menerima perjanjian atas nama organisasi Anda, pilih tab Perjanjian organisasi.
7. Pilih perjanjian, lalu pilih Unduh perjanjian.

Kotak dialog Terima NDA untuk mengunduh laporan muncul.

8. Sebelum Anda dapat mengunduh perjanjian yang Anda pilih, Anda harus terlebih dahulu menerima ketentuan Perjanjian AWS Artifact Kerahasiaan (AWS Artifact NDA).
 - a. Dalam kotak dialog Terima NDA untuk mengunduh laporan, tinjau AWS Artifact NDA.
 - b. (Opsional) Untuk mencetak salinan AWS Artifact NDA (atau menyimpannya sebagai PDF), pilih Cetak NDA.
 - c. Pilih Saya telah membaca dan menyetujui semua ketentuan NDA.
 - d. Untuk menerima AWS Artifact NDA dan mengunduh PDF perjanjian yang Anda pilih, pilih Terima NDA dan unduh.
9. Di penampil PDF, tinjau PDF perjanjian yang Anda unduh.
10. Di AWS Artifact konsol, dengan perjanjian yang dipilih, pilih Terima perjanjian.
11. Di kotak dialog Terima perjanjian, lakukan hal berikut:
 - a. Tinjau perjanjian.

- b. Pilih Saya menyetujui semua syarat dan ketentuan ini.
 - c. Pilih Terima perjanjian.
12. Pilih Terima untuk menerima perjanjian untuk akun Anda.

Mengakhiri perjanjian untuk Anda Akun AWS di AWS Artifact

Jika Anda menggunakan AWS Artifact konsol untuk [menerima perjanjian untuk satu Akun AWS](#), maka Anda dapat menggunakan konsol untuk mengakhiri perjanjian itu. Jika tidak menggunakan konsol, lihat [Perjanjian offline di AWS Artifact](#).

Izin yang diperlukan

[Untuk mengakhiri perjanjian, IAM dan pengguna federasi harus memiliki izin yang diperlukan.](#)

Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di AWS Artifact](#).

Untuk mengakhiri perjanjian online Anda dengan AWS

1. Buka AWS Artifact konsol di <https://console.aws.amazon.com/artifact/>.
2. Pada panel AWS Artifact navigasi, pilih Perjanjian.
3. Pilih tab Perjanjian akun.
4. Pilih perjanjian dan pilih Akhiri perjanjian.
5. Pilih semua kotak centang untuk menunjukkan bahwa Anda setuju untuk mengakhiri perjanjian.
6. Pilih Akhiri. Ketika diminta konfirmasi, pilih Akhiri.

Menerima perjanjian untuk organisasi Anda di AWS Artifact

Jika Anda adalah pemilik akun manajemen suatu AWS Organizations organisasi, maka Anda dapat menerima perjanjian dengan AWS atas nama semua Akun AWS di organisasi Anda.

Important

Sebelum Anda menerima perjanjian, sebaiknya Anda berkonsultasi dengan tim legal, privasi, dan kepatuhan Anda.

AWS Organizations memiliki dua set fitur yang tersedia: fitur penagihan terkonsolidasi dan semua fitur. Untuk digunakan AWS Artifact untuk organisasi Anda, organisasi yang Anda miliki harus diaktifkan untuk [semua fitur](#). Jika organisasi Anda dikonfigurasi hanya untuk tagihan terkonsolidasi, lihat [Mengaktifkan semua fitur di organisasi Anda](#) dalam Panduan Pengguna AWS Organizations .

Untuk menerima atau mengakhiri perjanjian organisasi, Anda harus masuk ke akun manajemen dengan AWS Artifact izin yang benar. Pengguna akun anggota yang memiliki `organizations:DescribeOrganization` izin dapat melihat perjanjian organisasi yang diterima atas nama mereka.

Untuk informasi selengkapnya, lihat [Mengelola akun AWS Organizations di organisasi dengan](#) di Panduan AWS Organizations Pengguna.

Izin yang diperlukan

Untuk menerima perjanjian, pemilik akun manajemen harus memiliki [izin](#) yang diperlukan.

Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di AWS Artifact](#).

Untuk menerima perjanjian bagi organisasi

1. Buka AWS Artifact konsol di <https://console.aws.amazon.com/artifact/>.
2. Di AWS Artifact dasbor, pilih Perjanjian.
3. Pilih tab Perjanjian organisasi.
4. Buka AWS Artifact konsol di <https://console.aws.amazon.com/artifact/>.
5. Di panel navigasi, pilih Perjanjian.
6. Pada halaman Perjanjian, lakukan salah satu hal berikut:
 - Untuk menerima perjanjian hanya untuk akun Anda, pilih tab Perjanjian akun.
 - Untuk menerima perjanjian atas nama organisasi Anda, pilih tab Perjanjian organisasi.
7. Pilih perjanjian, lalu pilih Unduh perjanjian.

Kotak dialog Terima NDA untuk mengunduh laporan muncul.

8. Sebelum Anda dapat mengunduh perjanjian yang Anda pilih, Anda harus terlebih dahulu menerima ketentuan Perjanjian AWS Artifact Kerahasiaan (AWS Artifact NDA).
 - a. Dalam kotak dialog Terima NDA untuk mengunduh laporan, tinjau AWS Artifact NDA.
 - b. (Opsional) Untuk mencetak salinan AWS Artifact NDA (atau menyimpannya sebagai PDF), pilih Cetak NDA.

- c. Pilih Saya telah membaca dan menyetujui semua ketentuan NDA.
 - d. Untuk menerima AWS Artifact NDA dan mengunduh PDF perjanjian yang Anda pilih, pilih Terima NDA dan unduh.
9. Di penampil PDF, tinjau PDF perjanjian yang Anda unduh.
 10. Di AWS Artifact konsol, dengan perjanjian yang dipilih, pilih Terima perjanjian.
 11. Di kotak dialog Terima perjanjian, lakukan hal berikut:
 - a. Tinjau perjanjian.
 - b. Pilih Saya menyetujui semua syarat dan ketentuan ini.
 - c. Pilih Terima perjanjian.
 12. Pilih Terima untuk menerima perjanjian untuk semua akun yang ada dan yang akan datang di organisasi Anda.

Mengakhiri perjanjian untuk organisasi Anda di AWS Artifact

Jika Anda menggunakan AWS Artifact konsol untuk [menerima perjanjian atas nama semua akun anggota di organisasi AWS Organizations](#), maka Anda dapat menggunakan konsol untuk mengakhiri perjanjian tersebut. Jika tidak, lihat [Perjanjian offline di AWS Artifact](#).

Jika akun anggota dihapus dari organisasi, maka akun anggota tersebut lebih lama dicakup oleh perjanjian organisasi. Sebelum menghapus akun anggota dari organisasi, administrator akun manajemen harus mengomunikasikan ini ke akun anggota sehingga mereka dapat menempatkan perjanjian baru jika perlu. Anda dapat melihat daftar perjanjian organisasi aktif di AWS Artifact konsol pada halaman Perjanjian, di bawah [Perjanjian organisasi](#).

Untuk informasi selengkapnya AWS Organizations, lihat [Mengelola akun di organisasi dengan AWS Organizations](#) di Panduan AWS Organizations Pengguna.

Izin yang diperlukan

Untuk mengakhiri perjanjian, pemilik akun manajemen harus memiliki [izin](#) yang diperlukan.

Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di AWS Artifact](#).

Untuk mengakhiri perjanjian organisasi online Anda dengan AWS

1. Buka AWS Artifact konsol di <https://console.aws.amazon.com/artifact/>.

2. Di AWS Artifact dasbor, pilih Perjanjian.
3. Pilih tab Perjanjian organisasi.
4. Pilih perjanjian dan pilih Akhiri perjanjian.
5. Pilih semua kotak centang untuk menunjukkan bahwa Anda setuju untuk mengakhiri perjanjian.
6. Pilih Akhiri. Ketika diminta konfirmasi, pilih Akhiri.

Perjanjian offline di AWS Artifact

Jika Anda memiliki perjanjian offline yang ada, AWS Artifact menampilkan perjanjian yang Anda terima secara offline. Sebagai contoh, konsol mungkin menampilkan Perjanjian Rekanan Bisnis (BAA) Offline dengan status Aktif. Status aktif menunjukkan bahwa perjanjian tersebut telah diterima. Untuk mengakhiri perjanjian offline, lihat pedoman pengakhiran dan instruksi yang disertakan dalam perjanjian Anda.

Lihat informasi yang lebih lengkap di [Identitas dan manajemen akses di AWS Artifact](#).

Mengkonfigurasi notifikasi email di AWS Artifact

Note

Konten halaman ini hanya berlaku untuk AWS [Wilayah](#) komersial, dan saat ini tidak berlaku untuk AWS GovCloud (US) Regions.

Anda dapat menggunakan AWS Artifact konsol untuk mengonfigurasi pemberitahuan email untuk pembaruan tentang perjanjian dan laporan di AWS Artifact. AWS Artifact mengirimkan notifikasi email ini menggunakan Notifikasi Pengguna AWS. Untuk menerima notifikasi AWS Artifact email, Anda harus terlebih dahulu memilih hub Notifikasi Pengguna AWS notifikasi di Notifikasi Pengguna konsol. Kemudian, di AWS Artifact konsol, Anda dapat membuat konfigurasi untuk pengaturan notifikasi, di mana Anda menentukan penerima notifikasi dan pemberitahuan mana yang mereka terima.

Untuk mengonfigurasi pemberitahuan AWS Artifact email, Anda harus memiliki izin yang diperlukan untuk AWS Artifact dan Notifikasi Pengguna AWS. Untuk informasi selengkapnya, lihat [Identitas dan manajemen akses di AWS Artifact](#).

Daftar Isi

- [Prasyarat: Pilih hub notifikasi di Notifikasi Pengguna](#)
- [Membuat konfigurasi untuk pengaturan AWS Artifact notifikasi](#)
- [Mengedit konfigurasi untuk pengaturan AWS Artifact notifikasi](#)
- [Menghapus konfigurasi untuk pengaturan AWS Artifact notifikasi](#)

Prasyarat: Pilih hub notifikasi di Notifikasi Pengguna

Sebelum Anda dapat menerima pemberitahuan AWS Artifact email, Anda harus terlebih dahulu membuka Notifikasi Pengguna konsol dan memilih hub notifikasi di Wilayah AWS tempat Anda ingin menyimpan Notifikasi Pengguna data Anda. Memilih hub notifikasi diperlukan untuk Notifikasi Pengguna AWS, yang AWS Artifact digunakan untuk mengirim notifikasi.

Untuk memilih hub notifikasi

1. Buka halaman [Hub notifikasi](#) Notifikasi Pengguna AWS konsol.

2. Pilih hub notifikasi di Wilayah AWS tempat Anda ingin menyimpan Notifikasi Pengguna AWS sumber daya Anda. Secara default, Notifikasi Pengguna data Anda disimpan di Wilayah AS Timur (Virginia N.). Notifikasi Pengguna mereplikasi data notifikasi Anda di seluruh Wilayah lain yang Anda pilih. Untuk informasi selengkapnya, lihat [dokumentasi hub notifikasi](#) di Panduan Notifikasi Pengguna AWS Pengguna.
3. Jangan pilih Save and continue (Simpan dan lanjutkan).

Membuat konfigurasi untuk pengaturan AWS Artifact notifikasi

Note

Konten halaman ini hanya berlaku untuk AWS [Wilayah](#) komersial, dan saat ini tidak berlaku untuk AWS GovCloud (US) Regions.

Setelah [memilih hub Notifikasi Pengguna notifikasi](#), Anda dapat membuat konfigurasi untuk pengaturan notifikasi di AWS Artifact konsol. Dalam konfigurasi yang Anda buat, Anda menentukan alamat email penerima yang ingin Anda terima AWS Artifact notifikasi. Anda juga menentukan pembaruan mana yang harus menerima pemberitahuan penerima tersebut, seperti pembaruan untuk AWS Artifact perjanjian, dan pembaruan untuk semua (atau sebagian dari) AWS Artifact laporan.

Untuk membuat konfigurasi

1. Buka halaman [Pengaturan notifikasi](#) AWS Artifact konsol.
2. Pilih Buat konfigurasi.
3. Pada halaman Buat konfigurasi, lakukan hal berikut:
 - Untuk menerima pemberitahuan untuk perjanjian, berdasarkan Perjanjian, tetap pilih Pembaruan pada AWS Perjanjian.
 - Untuk menerima pemberitahuan laporan, di bawah Laporan, simpan Pembaruan pada AWS Laporan yang dipilih.
 - a. Untuk menerima pemberitahuan untuk semua laporan, pilih Semua laporan.
 - b. Untuk menerima pemberitahuan hanya untuk laporan dalam kategori dan seri tertentu, pilih Subset laporan. Kemudian, pilih kategori dan seri yang Anda minati.
 - Di bawah Nama konfigurasi, masukkan Nama untuk konfigurasi Anda.

- Di bawah Email, untuk Penerima, masukkan daftar alamat email yang dipisahkan koma yang ingin Anda terima AWS Artifact email notifikasi.
- (Opsional) Untuk menambahkan tag ke konfigurasi notifikasi, perluas Tag, pilih Tambahkan tag baru, lalu masukkan tag sebagai pasangan nilai kunci. Untuk informasi selengkapnya tentang menandai Notifikasi Pengguna sumber daya, lihat [Menandai Notifikasi Pengguna AWS sumber daya Anda](#) di Notifikasi Pengguna AWS Panduan Pengguna.
- Pilih Buat konfigurasi.

Notifikasi Pengguna mengirimkan email verifikasi ke setiap alamat email penerima yang Anda berikan. Untuk memverifikasi alamat email, di email verifikasi, penerima harus memilih Verifikasi email. Hanya alamat email terverifikasi yang akan menerima AWS Artifact pemberitahuan.

Mengedit konfigurasi untuk pengaturan AWS Artifact notifikasi

Note

Konten halaman ini hanya berlaku untuk AWS [Wilayah](#) komersial, dan saat ini tidak berlaku untuk AWS GovCloud (US) Regions.

Setelah Anda [membuat konfigurasi](#) untuk pengaturan AWS Artifact notifikasi, Anda dapat mengedit konfigurasi kapan saja untuk mengubah pengaturan notifikasi Anda. Misalnya, untuk menambah atau menghapus penerima, ubah jenis notifikasi apa yang mereka terima, dan tambahkan atau hapus tag.

Untuk mengedit konfigurasi

1. Buka halaman [Pengaturan notifikasi](#) AWS Artifact konsol.
2. Pilih konfigurasi yang ingin Anda edit.
3. Pilih Edit.
4. Edit salah satu pilihan dan bidang konfigurasi. Setelah selesai, pilih Simpan perubahan.

Jika Anda telah menambahkan alamat email baru sebagai penerima notifikasi, Notifikasi Pengguna AWS kirimkan email verifikasi alamat email tersebut. Untuk memverifikasi alamat email, di email verifikasi, penerima harus memilih Verifikasi email. Hanya alamat email terverifikasi yang akan menerima AWS Artifact pemberitahuan.

Menghapus konfigurasi untuk pengaturan AWS Artifact notifikasi

Note

Konten halaman ini hanya berlaku untuk AWS [Wilayah](#) komersial, dan saat ini tidak berlaku untuk AWS GovCloud (US) Regions.

Jika Anda tidak lagi memerlukan [konfigurasi yang Anda buat](#) untuk pengaturan AWS Artifact notifikasi, maka Anda dapat menghapus konfigurasi di AWS Artifact konsol.

Untuk menghapus konfigurasi

1. Buka halaman [Pengaturan notifikasi](#) AWS Artifact konsol.
2. Pilih konfigurasi yang ingin Anda hapus.
3. Pilih Hapus.
4. Di kotak dialog Hapus konfigurasi, pilih Hapus.

Identitas dan manajemen akses di AWS Artifact

Saat mendaftar AWS, Anda memberikan alamat email dan kata sandi yang terkait dengan AWS akun Anda. Ini adalah kredensi root Anda, dan mereka menyediakan akses lengkap ke semua AWS sumber daya Anda, termasuk sumber daya untuk. AWS Artifact Namun, kami sangat menyarankan agar Anda tidak menggunakan akun root untuk akses sehari-hari. Kami juga menyarankan agar Anda tidak membagikan kredensial akun dengan orang lain untuk memberikan akses penuh ke akun Anda.

Alih-alih masuk ke AWS akun Anda dengan kredensi root atau berbagi kredensi Anda dengan orang lain, Anda harus membuat identitas pengguna khusus yang disebut pengguna IAM untuk diri sendiri dan bagi siapa saja yang mungkin memerlukan akses ke dokumen atau perjanjian. AWS Artifact Dengan pendekatan ini, Anda dapat memberikan informasi masuk berbeda untuk setiap pengguna, dan Anda dapat memberikan izin yang dibutuhkan tiap-tiap pengguna untuk bekerja dengan dokumen tertentu saja. Anda juga dapat memberikan izin yang sama kepada beberapa pengguna IAM dengan memberikan izin bagi grup IAM dan menambahkan pengguna IAM ke grup tersebut.

Jika Anda sudah mengelola identitas pengguna di luar AWS, Anda dapat menggunakan penyedia identitas IAM alih-alih membuat pengguna IAM. Untuk informasi selengkapnya, lihat [Penyedia dan federasi identitas](#) dalam Panduan Pengguna IAM.

Konten

- [Memberikan akses pengguna ke AWS Artifact](#)
- [Contoh kebijakan IAM untuk AWS Artifact di Wilayah komersial AWS](#)
- [Contoh kebijakan IAM untuk AWS Artifact in AWS GovCloud \(US\) Regions](#)
- [Menggunakan kebijakan AWS terkelola untuk AWS Artifact](#)
- [Menggunakan peran terkait layanan untuk AWS Artifact](#)
- [Menggunakan kunci kondisi IAM untuk laporan AWS Artifact](#)

Memberikan akses pengguna ke AWS Artifact

Selesaikan langkah-langkah berikut untuk memberikan izin kepada pengguna AWS Artifact berdasarkan tingkat akses yang mereka butuhkan.

Tugas

- [Langkah 1: Buat kebijakan IAM](#)

- [Langkah 2: Buat grup IAM dan lampirkan kebijakan](#)
- [Langkah 3: Buat pengguna IAM dan tambahkan ke grup](#)

Langkah 1: Buat kebijakan IAM

Sebagai administrator IAM, Anda dapat membuat kebijakan yang memberikan izin untuk AWS Artifact tindakan dan sumber daya.

Untuk membuat kebijakan IAM

Gunakan prosedur berikut untuk membuat kebijakan IAM yang dapat Anda gunakan untuk memberikan izin kepada pengguna dan grup IAM.

1. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pilih tab JSON.
5. Masukkan dokumen kebijakan. Anda dapat membuat kebijakan sendiri, atau Anda dapat menggunakan salah satu kebijakan dari [Contoh kebijakan IAM untuk AWS Artifact di Wilayah komersial AWS](#).
6. Pilih Tinjau Kebijakan. Validator kebijakan melaporkan kesalahan sintaksis.
7. Pada halaman Tinjau kebijakan, masukkan nama unik yang membantu Anda mengingat tujuan kebijakan. Anda juga dapat menambahkan deskripsi.
8. Pilih Buat kebijakan.

Langkah 2: Buat grup IAM dan lampirkan kebijakan

Sebagai administrator IAM, Anda dapat membuat grup dan melampirkan kebijakan yang Anda buat ke grup. Anda dapat menambahkan pengguna IAM ke grup kapan saja.

Untuk membuat grup IAM dan melampirkan kebijakan

1. Dalam panel navigasi, pilih Groups lalu pilih Create New Group.
2. Untuk Nama Grup, masukkan nama untuk grup Anda, lalu pilih Langkah Selanjutnya.
3. Di bidang pencarian, masukkan nama kebijakan yang Anda buat. Pilih kotak centang untuk kebijakan Anda, kemudian pilih Langkah Selanjutnya.

4. Tinjau nama grup dan kebijakan. Setelah semuanya selesai, pilih Buat Grup.

Langkah 3: Buat pengguna IAM dan tambahkan ke grup

Sebagai administrator IAM, Anda dapat menambahkan pengguna ke grup kapan saja. Ini memberikan kepada pengguna izin yang sama yang diberikan ke grup.

Untuk membuat pengguna IAM dan menambahkannya ke grup

1. Di panel navigasi, pilih Pengguna lalu pilih Tambahkan pengguna.
2. Untuk Nama pengguna, masukkan nama untuk satu atau lebih pengguna.
3. Pilih kotak centang di samping akses Konsol Manajemen AWS . Konfigurasi sandi yang dibuat secara otomatis atau kustom. Anda dapat memilih Pengguna harus membuat kata sandi baru saat masuk berikutnya untuk mengharuskan pengguna mengatur ulang kata sandi baru saat masuk pertama kali.
4. Pilih Selanjutnya: Izin.
5. Pilih Tambahkan pengguna ke grup lalu pilih grup yang Anda buat.
6. Pilih Selanjutnya: Tag. Anda dapat menambahkan tag secara opsional ke pengguna Anda.
7. Pilih Selanjutnya: Tinjau. Setelah semuanya selesai, pilih Buat pengguna.

Contoh kebijakan IAM untuk AWS Artifact di Wilayah komersial AWS

Anda dapat membuat kebijakan izin yang memberikan izin kepada pengguna IAM. Anda dapat memberi pengguna akses ke AWS Artifact laporan dan kemampuan untuk menerima dan mengunduh perjanjian atas nama satu akun atau organisasi.

Contoh kebijakan berikut menunjukkan izin yang dapat Anda tetapkan untuk pengguna IAM berdasarkan tingkat akses yang mereka butuhkan.

Kebijakan ini berlaku di AWS [Wilayah](#) komersial. Untuk kebijakan yang berlaku AWS GovCloud (US) Regions, lihat [Contoh kebijakan IAM untuk AWS Artifact AWS GovCloud \(US\) Regions](#)

- [Contoh kebijakan untuk mengelola AWS laporan dengan izin berbutir halus](#)
- [Contoh kebijakan untuk mengelola laporan pihak ketiga](#)
- [Contoh kebijakan untuk mengelola perjanjian](#)

- [Contoh kebijakan untuk diintegrasikan dengan AWS Organizations](#)
- [Contoh kebijakan untuk mengelola perjanjian untuk akun manajemen](#)
- [Contoh kebijakan untuk mengelola perjanjian organisasi](#)
- [Contoh kebijakan untuk mengelola notifikasi](#)

Example Contoh kebijakan untuk mengelola AWS laporan melalui izin berbutir halus

 Tip

Anda harus mempertimbangkan untuk menggunakan [kebijakan AWSArtifact ReportsReadOnlyAccess terkelola](#) alih-alih mendefinisikan kebijakan Anda sendiri.

Kebijakan berikut memberikan izin untuk mengunduh semua AWS laporan melalui izin berbutir halus.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk mengunduh hanya laporan AWS SOC, PCI, dan ISO melalui izin berbutir halus.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "artifact:ListReports"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "artifact:GetReportMetadata",
      "artifact:GetReport",
      "artifact:GetTermForReport",
      "artifact:ListReportVersions"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "artifact:ReportSeries": [
          "SOC",
          "PCI",
          "ISO"
        ],
        "artifact:ReportCategory": [
          "Certifications and Attestations"
        ]
      }
    }
  }
]
}

```

Example Contoh kebijakan untuk mengelola laporan pihak ketiga

 Tip

Anda harus mempertimbangkan untuk menggunakan [kebijakan AWSArtifact ReportsReadOnlyAccess terkelola](#) alih-alih mendefinisikan kebijakan Anda sendiri.

Laporan pihak ketiga dilambangkan dengan sumber daya IAM. `report`

Kebijakan berikut memberikan izin untuk semua fungsi laporan pihak ketiga.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk mengunduh laporan pihak ketiga.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk membuat daftar laporan pihak ketiga.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk melihat detail laporan pihak ketiga untuk semua versi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk melihat detail laporan pihak ketiga untuk versi tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

    "artifact:GetReportMetadata"
  ],
  "Resource": [
    "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
  ]
}
]
}

```

Tip

Anda harus mempertimbangkan untuk menggunakan [AWSArtifactAgreementsReadOnlyAccess](#) atau kebijakan yang [AWSArtifactAgreementsFullAccess dikelola](#) alih-alih mendefinisikan kebijakan Anda sendiri.

Example Contoh kebijakan untuk mengelola perjanjian

Kebijakan berikut memberikan izin untuk mengunduh semua perjanjian.

```

{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "arn:aws:artifact:::agreement/*"
  },
  {
    "Sid": "CustomerAgreementActions",
    "Effect": "Allow",
    "Action": [
      "artifact:GetCustomerAgreement"
    ],
    "Resource": "arn:aws:artifact::*:customer-agreement/*"
  }
]
}

```

Kebijakan berikut memberikan izin untuk menerima semua perjanjian.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}

```

Kebijakan berikut memberikan izin untuk mengakhiri semua perjanjian.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk melihat dan melaksanakan perjanjian tingkat akun.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}

```

Example Contoh kebijakan untuk diintegrasikan dengan AWS Organizations

Kebijakan berikut memberikan izin untuk membuat peran IAM yang AWS Artifact digunakan untuk berintegrasi dengan. AWS Organizations Akun manajemen organisasi Anda harus memiliki izin ini untuk memulai perjanjian organisasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
    },
  ],
}

```

```

    "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "artifact.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Kebijakan berikut memberikan izin untuk memberikan izin AWS Artifact untuk digunakan. AWS Organizations Akun manajemen organisasi Anda harus memiliki izin ini untuk memulai perjanjian organisasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

```

    }
  }
]
}

```

Example Contoh kebijakan untuk mengelola perjanjian bagi akun manajemen

Kebijakan berikut memberikan izin untuk mengelola perjanjian bagi akun manajemen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ],
}

```

```
{
  "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole",
    "iam:GetRole"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": [
        "artifact.amazonaws.com"
      ]
    }
  },
},
{
  "Sid": "EnableServiceTrust",
  "Effect": "Allow",
  "Action": [
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganization"
  ],
  "Resource": "*"
},
{
  "Sid": "EnableServiceTrustForArtifact",
  "Effect": "Allow",
  "Action": [
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": [
        "aws-artifact-account-sync.amazonaws.com"
      ]
    }
  }
}
]
```

Example Contoh kebijakan untuk mengelola perjanjian organisasi

Kebijakan berikut memberikan izin untuk mengelola perjanjian organisasi. Pengguna lain dengan izin yang diperlukan harus menyiapkan perjanjian organisasi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
    },
  ]
}
```

```

    "Resource": "*"
  }
]
}

```

Kebijakan berikut memberikan izin untuk melihat perjanjian organisasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "*"
  }
]
}

```

Example Contoh kebijakan untuk mengelola notifikasi

Kebijakan berikut memberikan izin lengkap untuk menggunakan AWS Artifact notifikasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications>DeleteEventRule",
        "notifications>DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications>ListChannels",
        "notifications>ListEventRules",
        "notifications>ListNotificationConfigurations",
        "notifications>ListNotificationHubs",
        "notifications>ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts>DeleteEmailContact",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts>ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
    },
  ],
}

```

```

    "Resource": [
      "*"
    ]
  }
]
}

```

Kebijakan berikut memberikan izin untuk mencantumkan semua konfigurasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

Kebijakan berikut memberikan izin untuk membuat konfigurasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",

```

```

    "notifications-contacts:CreateEmailContact",
    "notifications-contacts:SendActivationCode",
    "notifications:AssociateChannel",
    "notifications:CreateEventRule",
    "notifications:CreateNotificationConfiguration",
    "notifications:ListEventRules",
    "notifications:ListNotificationHubs",
    "notifications:TagResource",
    "notifications-contacts:ListEmailContacts"
  ],
  "Resource": [
    "*"
  ]
}
]
}

```

Kebijakan berikut memberikan izin untuk mengedit konfigurasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

```
    ]
  }
]
}
```

Kebijakan berikut memberikan izin untuk menghapus konfigurasi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk melihat detail konfigurasi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ]
  }
]
}

```

Kebijakan berikut memberikan izin untuk mendaftarkan atau membatalkan pendaftaran hub notifikasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

Contoh kebijakan IAM untuk AWS Artifact in AWS GovCloud (US) Regions

Kebijakan ini HANYA berlaku di AWS GovCloud (US) Regions. Untuk kebijakan yang berlaku untuk AWS [Wilayah](#) komersial, lihat [Contoh kebijakan IAM untuk AWS Artifact Wilayah komersial AWS](#)

Anda dapat membuat kebijakan izin yang memberikan izin kepada pengguna IAM. Anda dapat memberi pengguna akses ke AWS Artifact laporan dan kemampuan untuk menerima dan mengunduh perjanjian atas nama satu akun atau organisasi.

Contoh kebijakan berikut menunjukkan izin yang dapat Anda tetapkan untuk pengguna IAM berdasarkan tingkat akses yang mereka butuhkan.

- [Contoh kebijakan untuk mengelola laporan AWS](#)
- [Contoh kebijakan untuk mengelola perjanjian](#)

- [Contoh kebijakan untuk diintegrasikan dengan AWS Organizations](#)
- [Contoh kebijakan untuk mengelola perjanjian untuk akun manajemen](#)
- [Contoh kebijakan untuk mengelola perjanjian organisasi](#)

Example Contoh kebijakan untuk mengelola laporan

Kebijakan berikut memberikan izin untuk mengunduh semua laporan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan berikut memberikan izin untuk mengunduh hanya laporan SOC, PCI, dan ISO.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
```

```

    "Effect": "Allow",
    "Action": [
      "artifact:GetReportMetadata",
      "artifact:GetReport",
      "artifact:GetTermForReport",
      "artifact:ListReportVersions"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "artifact:ReportSeries": [
          "SOC",
          "PCI",
          "ISO"
        ],
        "artifact:ReportCategory": [
          "Certifications and Attestations"
        ]
      }
    }
  ]
}

```

Example Contoh kebijakan untuk mengelola perjanjian

Kebijakan berikut memberikan izin untuk mengunduh semua perjanjian. Pengguna IAM juga harus memiliki izin ini untuk menerima perjanjian.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

```

    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}

```

Kebijakan berikut memberikan izin untuk menerima semua perjanjian.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",

```

```

        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
    ],
    "Resource": "arn:aws-us-gov:artifact:::agreement/*"
}
]
}

```

Kebijakan berikut memberikan izin untuk mengakhiri semua perjanjian.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}

```

Kebijakan berikut memberikan izin untuk melihat dan melaksanakan perjanjian tingkat akun.

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```

{
  "Sid": "ListAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:ListAgreements",
    "artifact:ListCustomerAgreements"
  ],
  "Resource": "*"
},
{
  "Sid": "AWSAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:GetAgreement",
    "artifact:AcceptNdaForAgreement",
    "artifact:GetNdaForAgreement",
    "artifact:AcceptAgreement"
  ],
  "Resource": "arn:aws-us-gov:artifact:::agreement/*"
},
{
  "Sid": "CustomerAgreementActions",
  "Effect": "Allow",
  "Action": [
    "artifact:GetCustomerAgreement",
    "artifact:TerminateAgreement"
  ],
  "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
}
]
}

```

Example Contoh kebijakan untuk diintegrasikan dengan AWS Organizations

Kebijakan berikut memberikan izin untuk membuat peran IAM yang AWS Artifact digunakan untuk berintegrasi dengan. AWS Organizations Akun manajemen organisasi Anda harus memiliki izin ini untuk memulai perjanjian organisasi.

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```

{
  "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole",
    "iam:GetRole"
  ],
  "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": [
        "artifact.amazonaws.com"
      ]
    }
  }
}

```

Kebijakan berikut memberikan izin untuk memberikan izin AWS Artifact untuk digunakan. AWS Organizations Akun manajemen organisasi Anda harus memiliki izin ini untuk memulai perjanjian organisasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
    }
  ]
}

```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "aws-artifact-account-sync.amazonaws.com"
        ]
      }
    }
  ]
}

```

Example Contoh kebijakan untuk mengelola perjanjian bagi akun manajemen

Kebijakan berikut memberikan izin untuk mengelola perjanjian bagi akun manajemen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",

```

```

    "Effect": "Allow",
    "Action": [
      "artifact:GetCustomerAgreement",
      "artifact:TerminateAgreement"
    ],
    "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
  },
  {
    "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole",
      "iam:GetRole"
    ],
    "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "artifact.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "EnableServiceTrust",
    "Effect": "Allow",
    "Action": [
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganization"
    ],
    "Resource": "*"
  },
  {
    "Sid": "EnableServiceTrustForArtifact",
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "aws-artifact-account-sync.amazonaws.com"
        ]
      }
    }
  }
}

```

```

    ]
  }
}
]
}

```

Example Contoh kebijakan untuk mengelola perjanjian organisasi

Kebijakan berikut memberikan izin untuk mengelola perjanjian organisasi. Pengguna lain dengan izin yang diperlukan harus menyiapkan perjanjian organisasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeOrganization"
    ],
    "Resource": "*"
  }
]
}

```

Kebijakan berikut memberikan izin untuk melihat perjanjian organisasi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ]
    }
  ]
}

```

```
    ],
    "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeOrganization"
    ],
    "Resource": "*"
  }
]
```

Menggunakan kebijakan AWS terkelola untuk AWS Artifact

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: [AWSArtifactReportsReadOnlyAccess](#)

Anda dapat melampirkan kebijakan `AWSArtifactReportsReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan *read-only* izin yang memungkinkan daftar, melihat, dan mengunduh laporan.

Detail izin

Kebijakan ini mencakup izin berikut.

- `artifact`— Memungkinkan kepala sekolah untuk membuat daftar, melihat, dan mengunduh laporan dari. AWS Artifact

AWS kebijakan terkelola: [AWSArtifactAgreementsReadOnlyAccess](#)

Anda dapat melampirkan kebijakan `AWSArtifactAgreementsReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan *read-only* akses untuk membuat daftar perjanjian layanan AWS Artifact dan mengunduh perjanjian yang diterima. Ini juga mencakup izin untuk membuat daftar serta menjelaskan detail organisasi. Selain itu, kebijakan menyediakan kemampuan untuk memeriksa apakah peran terkait layanan yang diperlukan ada.

Detail izin

Kebijakan ini mencakup izin berikut.

- `artifact`— Memungkinkan kepala sekolah untuk membuat daftar semua perjanjian dan untuk melihat perjanjian yang diterima dari. AWS Artifact
- `iam`— Memungkinkan kepala sekolah untuk memeriksa apakah peran terkait layanan yang diperlukan ada.
- `organizations`— Memungkinkan kepala sekolah untuk menggambarkan organisasi saat ini dan membuat daftar akses layanan untuk organisasi itu.

AWS kebijakan terkelola: [AWSArtifactAgreementsFullAccess](#)

Anda dapat melampirkan kebijakan `AWSArtifactAgreementsFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan *full* izin untuk membuat daftar, mengunduh, menerima, dan mengakhiri perjanjian Artifact AWS. Ini juga mencakup izin untuk membuat daftar dan mengaktifkan akses layanan AWS di AWS Organizations layanan, serta menjelaskan detail organisasi. Selain itu, kebijakan menyediakan kemampuan untuk memeriksa apakah peran terkait layanan yang diperlukan ada dan membuatnya jika tidak.

Detail izin

Kebijakan ini mencakup izin berikut.

- `artifact`— Memungkinkan kepala sekolah untuk membuat daftar, mengunduh, menerima, dan mengakhiri perjanjian dari. AWS Artifact
- `iam`— Memungkinkan kepala sekolah untuk memeriksa apakah peran terkait layanan yang diperlukan ada, dan membuatnya jika tidak.
- `organizations`— Memungkinkan kepala sekolah untuk menggambarkan organisasi saat ini dan untuk `list/enable` melayani akses untuk organisasi itu.

AWS Artifact pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Artifact sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman [Riwayat AWS Artifact dokumen](#).

Ubah	Deskripsi	Tanggal
AWSArtifactReportsReadOnlyAccess — Pembaruan ke kebijakan yang sudah ada	AWS Artifact menambahkan <code>artifact:ListReportVersions</code> izin untuk mengizinkan daftar versi laporan.	2025-12-15
Kebijakan terkelola Perjanjian AWS yang diperbarui	Kebijakan <code>AWSArtifactAgreementsFullAccess</code> terkelola yang diperbarui	2025-10-16

Ubah	Deskripsi	Tanggal
	untuk cakupan organisasi: EnableAWSServiceAccess izin hingga AWS Artifact prinsip layanan. Ini tidak memengaruhi fungsionalitas kebijakan terkelola.	
Kebijakan terkelola AWS Reports yang diperbarui	Kebijakan AWSArtifact ReportsReadOnlyAccess terkelola yang diperbarui untuk menghapus izin artefact:get.	2025-03-21
Memperkenalkan kebijakan terkelola Perjanjian AWS	Kebijakan yang diperkenalkan AWSArtifact Agreement sReadOnlyAccess dan AWSArtifact Agreement sFullAccess dikelola.	2024-11-21
AWS Artifact mulai melacak perubahan	AWS Artifact mulai melacak perubahan untuk kebijakan yang AWS dikelola dan diperkenalkan AWSArtifactReportsReadOnlyAccess.	2023-12-15

Menggunakan peran terkait layanan untuk AWS Artifact

AWS Artifact menggunakan AWS Identity and Access Management peran [terkait layanan](#) (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Artifact Service-linked peran telah ditentukan sebelumnya oleh AWS Artifact dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Artifact lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Artifact mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Artifact dapat mengambil perannya. Izin-izin yang

ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi AWS Artifact sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS layanan yang bekerja dengan IAM](#) dan cari layanan yang memiliki Ya di kolom peran. Service-linked Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Service-linked izin peran untuk AWS Artifact

AWS Artifact menggunakan peran terkait layanan bernama `AWSServiceRoleForArtifact`. Memungkinkan AWS Artifact untuk mengumpulkan informasi tentang organisasi melalui AWS Organizations

Peran `AWSServiceRoleForArtifact` terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `artifact.amazonaws.com`

Kebijakan izin peran bernama `AWSArtifactServiceRolePolicy` memungkinkan AWS Artifact untuk menyelesaikan tindakan berikut pada `organizations` sumber daya.

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

Membuat peran terkait layanan untuk AWS Artifact

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuka tab Perjanjian organisasi di akun manajemen organisasi dan memilih tautan Memulai di Konsol Manajemen AWS, AWS Artifact buat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuka tab

Perjanjian organisasi di akun manajemen organisasi dan memilih tautan Memulai, AWS Artifact buat peran terkait layanan untuk Anda lagi.

Menyunting peran terkait layanan untuk AWS Artifact

AWS Artifact tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForArtifact` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Artifact

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

Note

Jika AWS Artifact layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus AWS Artifact sumber daya yang digunakan oleh `AWSServiceRoleForArtifact`

1. Kunjungi tabel 'Perjanjian Organisasi' di konsol AWS Artifact
2. Mengakhiri perjanjian Organisasi yang aktif

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran `AWSServiceRoleForArtifact` terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk AWS Artifact peran terkait layanan

AWS Artifact tidak mendukung penggunaan peran terkait layanan di setiap Wilayah tempat layanan tersedia. Anda dapat menggunakan `AWSServiceRoleForArtifact` peran di Wilayah berikut.

Nama wilayah	Identitas wilayah	Support di AWS Artifact
US East (Northern Virginia)	us-east-1	Ya
US East (Ohio)	us-east-2	Tidak
AS Barat (California Utara)	us-west-1	Tidak
AS Barat (Oregon)	us-west-2	Ya
Africa (Cape Town)	af-south-1	Tidak
Asia Pasifik (Hong Kong)	ap-east-1	Tidak
Asia Pasifik (Jakarta)	ap-southeast-3	Tidak
Asia Pasifik (Mumbai)	ap-south-1	Tidak
Asia Pacific (Osaka)	ap-northeast-3	Tidak
Asia Pasifik (Seoul)	ap-northeast-2	Tidak
Asia Pasifik (Singapura)	ap-southeast-1	Tidak
Asia Pasifik (Sydney)	ap-southeast-2	Tidak
Asia Pasifik (Tokyo)	ap-northeast-1	Tidak
Kanada (Pusat)	ca-central-1	Tidak
Eropa (Frankfurt)	eu-central-1	Tidak
Eropa (Irlandia)	eu-west-1	Tidak
Eropa (London)	eu-west-2	Tidak
Europe (Milan)	eu-south-1	Tidak

Nama wilayah	Identitas wilayah	Support di AWS Artifact
Eropa (Paris)	eu-west-3	Tidak
Eropa (Stockholm)	eu-north-1	Tidak
Timur Tengah (Bahrain)	me-south-1	Tidak
Timur Tengah (UAE)	me-central-1	Tidak
Amerika Selatan (Sao Paulo)	sa-east-1	Tidak
AWS GovCloud (US-East)	us-gov-east-1	Tidak
AWS GovCloud (US-West)	us-gov-west-1	Ya

Menggunakan kunci kondisi IAM untuk laporan AWS Artifact

Anda dapat menggunakan kunci kondisi IAM untuk memberikan akses halus ke laporan AWS Artifact, berdasarkan kategori dan seri laporan tertentu.

Contoh kebijakan berikut menunjukkan izin yang dapat Anda tetapkan ke pengguna IAM berdasarkan kategori dan seri laporan tertentu.

Example Contoh kebijakan untuk mengelola akses baca AWS laporan

AWS Artifact laporan dilambangkan dengan sumber daya IAM, `report`

Kebijakan berikut memberikan izin untuk membaca semua AWS Artifact laporan di bawah `Certifications and Attestations` kategori.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

```

},
{
  "Effect": "Allow",
  "Action": [
    "artifact:GetReport",
    "artifact:GetReportMetadata",
    "artifact:GetTermForReport"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "artifact:ReportCategory": "Certifications and Attestations"
    }
  }
}
]
}

```

Kebijakan berikut memungkinkan Anda memberikan izin untuk membaca semua AWS Artifact laporan di bawah SOC seri.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {

```

```

        "StringEquals": {
            "artifact:ReportSeries": "SOC",
            "artifact:ReportCategory": "Certifications and Attestations"
        }
    }
}
]
}

```

Kebijakan berikut memungkinkan Anda memberikan izin untuk membaca semua AWS Artifact laporan di bawah Certifications and Attestations kategori, dan SOC seri.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}

```

Pencatatan panggilan AWS Artifact API dengan AWS CloudTrail

AWS Artifact terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS Artifact. CloudTrail menangkap panggilan API untuk AWS Artifact sebagai acara. Panggilan yang diambil termasuk panggilan dari AWS Artifact konsol dan panggilan kode ke operasi AWS Artifact API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk AWS Artifact. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Artifact, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

AWS Artifact informasi di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di AWS Artifact, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan Riwayat CloudTrail acara](#).

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk AWS Artifact, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran umum untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)

- [Menerima file CloudTrail log dari beberapa wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

AWS Artifact mendukung pencatatan tindakan berikut sebagai peristiwa dalam file CloudTrail log:

- [ListReports](#)
- [GetAccountSettings](#)
- [GetReportMetadata](#)
- [GetReport](#)
- [GetTermForReport](#)
- [PutAccountSettings](#)
- [AcceptAgreement](#)
- [AcceptNdaForAgreement](#)
- [GetAgreement](#)
- [GetCustomerAgreement](#)
- [GetNdaForAgreement](#)
- [ListAgreements](#)
- [ListCustomerAgreements](#)
- [TerminateAgreement](#)

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan itu dibuat dengan kredensial pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#) .

Memahami entri file AWS Artifact log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan GetReportMetadata tindakan.

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httpplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
```

```
"eventVersion": "1.03",
"userIdentity": {
  "type": "IAMUser",
  "principalId": "A1B2C3D4E5F6G7EXAMPLE",
  "arn": "arn:aws:iam::999999999999:user/myUserName",
  "accountId": "999999999999",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "myUserName"
},
"eventTime": "2015-03-18T19:04:42Z",
"eventSource": "artifact.amazonaws.com",
"eventName": "GetReportMetadata",
"awsRegion": "us-east-1",
"sourceIPAddress": "127.0.0.1",
"userAgent": "Python-httpplib2/0.8 (gzip)",
"requestParameters": {
  "reportId": "report-f1DIWBmGa2Lhsadg"
},
"responseElements": null,
"requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
"eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
"eventType": "AwsApiCall",
"recipientAccountId": "999999999999"
}
]
}
```

Riwayat dokumen untuk AWS Artifact

Tabel berikut menyediakan riwayat AWS Artifact rilis dan perubahan terkait pada Panduan AWS Artifact Pengguna.

Perubahan	Deskripsi	Tanggal
Izin yang diperbarui untuk API ListReportVersions	Contoh kebijakan IAM yang diperbarui, misalnya kebijakan GovCloud IAM , kebijakan AWSArtifactReportsReadOnlyAccess terkelola, dan instruksi pengunduhan laporan untuk menyertakan artifact: ListReportVersions izin dan dukungan untuk mengunduh versi laporan guna mengakomodasi API baru ListReportVersions .	Desember 15, 2025
Kebijakan AWSArtifactAgreementsFullAccess terkelola yang diperbarui	Kebijakan AWSArtifactReportsReadOnlyAccess terkelola yang diperbarui untuk cakupan <code>organizations:EnableAWSServiceAccess</code> izin hingga AWS Artifact prinsip layanan. Ini tidak memengaruhi fungsionalitas kebijakan terkelola.	Oktober 16, 2025
Pembaruan Pemberitahuan Pengakhiran Tindakan IAM	Memperbarui pemberitahuan penghentian tindakan IAM untuk artifact: DownloadAgreement dan	Juli 1, 2025

	<p><code>artifact:Get</code> di partisi. AWS GovCloud (US)</p>	
<p>Fine-grained izin untuk AWS Artifact di AWS GovCloud (US) Regions</p>	<p>Kebijakan yang diperbarui dan diperluas untuk digunakan AWS Artifact AWS GovCloud (US) Regions, sambil menghapus catatan tentang batasan karena AWS Artifact fungsionalitas sekarang lebih luas berlaku di semua wilayah.</p>	<p>Maret 31, 2025</p>
<p>Kebijakan AWSArtifactReportReadOnlyAccess terkelola yang diperbarui</p>	<p>Kebijakan AWSArtifactReportsReadOnlyAccess terkelola yang diperbarui untuk menghapus izin <code>artifact:get</code>.</p>	<p>Maret 21, 2025</p>
<p>Contoh kebijakan untuk AWS Artifact di AWS GovCloud (US) Regions</p>	<p>Menambahkan contoh kebijakan untuk digunakan AWS Artifact AWS GovCloud (US) Regions, dan mencatat halaman mana yang tidak berlaku untuk digunakan AWS Artifact AWS GovCloud (US) Regions.</p>	<p>Desember 6, 2024</p>
<p>Fine-grained izin untuk pelaksanaan perjanjian, AWSArtifactAgreementsFullAccess dan kebijakan AWSArtifactAgreementsReadOnlyAccess terkelola</p>	<p>Mengaktifkan akses berbutir halus untuk pelaksanaan AWS Artifact perjanjian dan kebijakan yang diluncurkan AWSArtifactAgreementsFullAccess dan AWSArtifactAgreementsReadOnlyAccess AWS dikelola.</p>	<p>November 21, 2024</p>

Fine-grained akses laporan dan kebijakan AWSArtifactReportReadOnlyAccess terkelola	Mengaktifkan akses halus ke AWS Artifact laporan, mengaktifkan kunci kondisi laporan, dan meluncurkan AWSArtifactReports ReadOnlyAccess kebijakan terkelola.	15 Desember 2023
AWS Artifact peran terkait layanan	Menambahkan dokumentasi peran terkait layanan dan kebijakan contoh yang diperbarui untuk AWS Artifact dan AWS Organizations integrasi.	26 September 2023
Pemberitahuan	Menerbitkan dokumentasi untuk mengelola notifikasi, dan membuat pembaruan yang relevan pada Referensi AWS Artifact API, dokumentasi CloudTrail pencatatan, dan halaman Manajemen Identitas dan akses.	1 Agustus 2023
Third-party laporan - Umumnya tersedia	Menambahkan dokumentasi referensi API dan dokumentasi CloudTrail logging, dan membuat laporan pihak ketiga tersedia secara umum.	27 Januari 2023

Third-party laporan (Pratinjau)	Meluncurkan laporan kepatuhan vendor perangkat lunak independen (ISV) yang menjual produk mereka. AWS Marketplace Menambahkan contoh kebijakan ke halaman Identitas dan manajemen akses untuk laporan pihak ketiga.	30 November 2022
Keamanan	Menambahkan bagian ke halaman Identitas dan manajemen akses untuk pencegahan wakil yang membingungkan.	Desember 20, 2021
Laporan	Menghapus perjanjian kerahasiaan dan memperkenalkan syarat dan ketentuan untuk unduhan laporan.	17 Desember 2020
Halaman rumah dan pencarian	Menambahkan halaman beranda layanan dan bilah pencarian pada halaman laporan dan perjanjian.	15 Mei 2020
AWS GovCloud (US) peluncuran	Diluncurkan AWS Artifact di AWS GovCloud (US) Regions.	7 November 2019
AWS Organizations perjanjian	Menambahkan dukungan untuk mengelola perjanjian untuk organisasi.	20 Juni 2018
Perjanjian	Menambahkan dukungan untuk mengelola AWS Artifact perjanjian.	17 Juni 2017

[Rilis awal](#)

Rilis ini memperkenalkan AWS 30 November 2016
Artifact.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.